GROUP BASED CRYPTOGRAPHY

DELARAM KAHROBAEI (NEW YORK)

The National Security Agency (NSA) in August 2015 announced plans to transition to post-quantum algorithms (i.e. resistant to a quantum computers). Quantum computers work with q-bits instead of bits that classical computers work with. Shortly after that, the National Institute of Standards and Technology (NIST) announced a worldwide competition for quantum-resistant public-key algorithms. The academic and industrial communities around the world including France, have suggested as quantum-resistant primitives: Lattice-based, Multivariate, Code-based, Hash-based, Isogeny-based and Group-based primitives.

Group-based cryptography has been an active area for over a decade, and it has some promises to be one of the solutions for this call.

Traditionally number-theoretic problems have been used for cryptography, for example RSA is based on the difficulty of prime factorization. The group-based cryptographers aim to use algorithmic group theoretic problems for secure platforms for cryptology.

The one which was proposed to NIST is by the SecureRF company based in Connecticut, and has among its founders a number theorist (Goldfeld) and two group theorists (Anshel and Anshel). They proposed a digital signature using a hard algorithmic problem in braid groups, namely the conjugacy problem. There has been other cryptosystems based on group theoretic problems for example Chatterji-Kahrobaei-Lu recently proposed hyperbolic groups for cryptographic purposes.

In this mini-course I will focus on some ideas of group-based primitives. I will explore some of the proposed cryptographic schemes and discuss open problems. I will recall basic ideas of cryptography and some group theory background for our purpose. The course is accessible to MS and PhD students in Mathematics and Computer science and perhaps some advanced undergraduate students.

August 27 and 28th (Monday and Tuesday) 10-12

Please e-mail Indira Chatterji indira@unice.fr if you want to come: the course might be cancelled if there is less than 3 students